UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,695	08/31/2001	Sridhar Dathathraya	SLA1055	2135

55286 7590 12/30/2005

SHARP LABORATORIES OF AMERICA, INC.
C/O LAW OFFICE OF GERALD MALISZEWSKI
P.O. BOX 270829
SAN DIEGO, CA 92198-2829

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/944,695
Filing Date: August 31, 2001
Appellant(s): DATHATHRAYA, SRIDHAR

Sharp Laboratories of America – Gerald Maliszewski, ESQ

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed October 5, 2005 appealing from the Office action mailed June 27, 2005.

(1) Real Party in Interest

The real party in interest is Sharp Laboratories of America, Inc., as assignee of the present application.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

No evidence is relied upon by the examiner in the rejection of the claims under appeal.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-8, 10-25, and 27-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mazzagatte, et al (US 6,862,583), and further in view of DeBry (US 6,385,728).

As per claim 12, broadly claims receiving from the server a document that was encrypted with a public key whereby accepting a private key corresponding to the public key of the encrypted document and using the private key to decrypt and print the documents.

Mazzagatte teach a method for receiving encrypted documents spooled from a file server (col.6, lines 64-65) wherein the printer 50 is connected to the network 100 that is able to receive email messages containing print job related

information (col.6, lines 25-28). Figure 1, shows the printer is connected to and in communication to the network. Mazzagatte reference describing more on the symmetric key technique and less on what is involved in an asymmetric key technique. Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric (public/private key) algorithms (col.8, lines 38-40 and col.9, lines 15-16), Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source, which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify that the user has correct access privileges (col.5, lines 51-65). Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15). Part of DeBry's invention involves authenticating the printer prior to allowing the printer to receiving encrypted documents. Thus, DeBry has an added security measure to make sure the printer is trusted before transmitting the files and thereafter

the server have the option using a secret key or a public key to encrypt prior to sending an encrypted file to the user whereby the user decrypts the file using the appropriate key **(col.10, lines 16-21).** The appropriate key of an asymmetric key scheme can obviously be a private key if the received public key is used for encryption.

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer because to prevent unauthorized printing and spoofing.

As per claim 13: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discusses decrypting the documents with the private key includes operating the printer in response to publicly distributed printer driver encryption software.

As per claim 14: See Mazzagatte on col.8, lines 32-40 and col.9, line 52-55; discusses the printer has a card reader to read code from SMART cards; and, wherein accepting a private key includes using the code read by the printer card reader as the private key.

As per claim 15: See Mazzagatte on col.8, lines 19-41 and col.10, lines 4-

18; discusses storing the private keys in the printer; creating a table in the printer to cross-reference private keys with alpha-numeric codes; and, wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code as the private key.

As per claim 16: See Mazzagatte on col.5, lines 53-65 and col.6, line 62-col.7, line 5; discussing spooling the encrypted documents from the file server into a printer memory; and, wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

As per claim 17: See Mazzagatte on col.7, lines 3-56 and col.9, lines 26-34; discusses in response to accepting the private key, generating a list of documents encrypted with a corresponding public key; creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document ; and, wherein printing the documents includes printing the documents in response to selecting a document.

As per claim 18: See Mazzagatte on col.4, lines 37-40; discusses receiving documents encrypted with a public key includes receiving encrypted documents transmitted as a facsimile (FAX) transmission; and, wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

As per claim 29:

Mazzagatte discloses a secure communications network-connected printer, the printer comprising:

a network connection to receive documents from the file server **(col.6, lines 20-28 and col.6, line Figure 1)** encrypted with a public key; **(col.8, lines 39 and 66-67)**

an input to accept a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.9, lines 13-20)**

an decryption application to decrypt the documents with the private key; and, an output to supply a printout of the decrypted documents; and **(col.10, lines 31-39)**

an output to supply a printout of the decrypted documents.

The server of Mazzagatte is a print node (col.7, lines 39-44) which may be a gateway to one or multiple printers (col.10, lines 43-44) or basically a file server (col.4, lines 31-34), where the print node server receives the encrypted data and identification information using public/private key encryption (col.4, lines 40-42) and sends the encrypted data with the private key (col.10, lines 31-33) to the printer for printing (col.6, lines 63-65). The print node and the printer communicates with one another such that the print node indicates the print job information for the printer to determine which recipient is to receive the printouts from the print queue (col.10, lines 13-14). Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric

(public/private key) algorithms (col.8, lines 38-40 and col.9, lines 15-16), Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source, which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify that the user has correct access privileges (col.5, lines 51-65). Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15). Part of DeBry's invention involves authenticating the printer prior to allowing the printer to receiving encrypted documents. Thus, DeBry has an added security measure to make sure the printer is trusted before transmitting the files and thereafter the server have the option using a secret key or a public key to encrypt prior to sending an encrypted file to the user whereby the user decrypts the file using the appropriate key **(col.10, lines 16-21).** The appropriate key of an asymmetric

key scheme can obviously be a private key if the received public key is used for encryption.

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer because to prevent unauthorized printing and spoofing.

As per claim 30: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discussing the decryption application is responsive to publicly distributed printer driver encryption software.

As per claim 31: See Mazzagatte on col.8, lines 32-40 and col.9, line 56; discussing the private key input is a card reader to read code from SMART cards.

As per claim 32: See col.4, lines 39-41 and col.10, lines 4-18; the private key input is a keyboard interface to accept an alpha-numeric code; and, the printer further comprising: a memory to store the private keys; a memory to store a table cross-referencing private keys with alpha-numeric codes; and, wherein private key input uses the private key referenced by the alpha-numeric code entered at the printer keyboard.

As per claim 33: See Mazzagatte on col.6, lines 20-21 and col.6, line 62-col.7, line 5; a memory to spool the encrypted documents from the file server, and wherein decryption application retrieves the encrypted documents from printer memory for decryption.

As per claim 34: Mazzagatte discusses the printer of claim 29 further comprising a display having an input **(col.9, lines 65-66)** wherein the decryption application creates a graphical user interface (GUI) dialog box application on the display to invoke the selection of an encrypted document **(col.9, lines 63-66)**, the GUI generating a list of documents encrypted with a corresponding public key, in response to accepting the private key **(col.9, lines 26-34 and 10, lines 31-37),** and wherein the documents are decrypted and printed in response to the documents being selected from the GUI. **(col.7, lines 33-45)**

As per claim 35: See Mazzagatte on col.4, lines 37-40 and col.7, lines 33-45; the network connection is a telephone connection and the encrypted documents are facsimile (FAX) transmissions; and wherein the printer decrypts the encrypted FAX transmission.

As per claim 1:

Mazzagatte, et al. discloses in a network of connected devices, a communications security method comprising:

encrypting documents **(col.8, lines 14-15)** with a public key; **(col.8, lines 39 and 66-67)**

spooling the encrypted documents to a network connected file server; **(col.6, lines 20-21 and col.6, line 62 – col.7, line 5)**

notifying the printer of encrypted documents spooled on the network file server; **(col.9, lines 26-31)**

at the printer, accepting a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.10, lines 26-28)**

following the acceptance of the private key, transmitting the encrypted documents to a network connected printer; **(col.10, lines 29-30 and col.11, lines 50-53)**

decrypting the documents with the private key; and, **(col.10, lines 31-39)**

printing the decrypted documents. **(col.11, lines 54-57)**

The server of Mazzagatte is a print node (col.7, lines 39-44) which may be a gateway to one or multiple printers (col.10, lines 43-44) or basically a file server (col.4, lines 31-34), where the print node server receives the encrypted data and identification information using public/private key encryption (col.4, lines 40-42) and sends the encrypted data with the private key (col.10, lines 31-33) to the printer for printing (col.6, lines 63-65). The print node and the printer communicates with one another such that the print node indicates the print job information for the printer to determine which recipient is to receive the printouts from the print queue (col.10, lines 13-14). Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric

(public/private key) algorithms (col.8, lines 38-40 and col.9, lines 15-16), Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source, which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify that the user has correct access privileges (col.5, lines 51-65). Part of DeBry's invention involves authenticating the printer prior to allowing the printer to receiving encrypted documents. Thus, DeBry has an added security measure to make sure the printer is trusted before transmitting the files and thereafter the server have the option using a secret key or a public key to encrypt prior to sending an encrypted file to the user whereby the user decrypts the file using the appropriate key **(col.10, lines 16-21).** The appropriate key of an asymmetric key scheme can obviously be a private key if the received public key is used for encryption. Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to

decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15).

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer because to prevent unauthorized printing and spoofing.

As per claim 2: See Mazzagatte on col.4, lines 9-10 and col.6, line 62 – col.7, line 5; discusses encrypting the documents with a public key includes encrypting the documents at a network-connected computer having a public key encryption application wherein transmitting the encrypted documents to a network-connected printer includes transmitting the encrypted documents between the computer, file server, and the printer, through a network.

As per claim 3: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discussing supplying the printer driver encryption software to the computer.

As per claim 4: See Mazzagatte on col.4, lines 54-58 and col.7, lines 33-67; discusses supplying an application to optionally encrypt documents in response to the application, creating a graphical user interface (GUI) dialog box

to invoke the document encryption option, and in response to invoking the document encryption option, creating a graphical user interface (GUI) dialog box to request and accept public key information.

As per claim 5: See Mazzagatte on col.9, lines 13-20; discusses generating a plurality of public keys with corresponding private keys, distributing the public keys universally to network-connected computers, and selectively distributing the private keys.

As per claim 6: See Mazzagatte on col.8, lines 32-40 and col.9, line 52-55; discussing the printer has a card reader to read code from SMART cards, wherein selectively distributing the private keys includes distributing the private keys as SMART cards, and wherein accepting a private key includes using the code read by the printer card reader.

As per claim 7: See Mazzagatte on col.8, lines 19-41 and col.10, lines 4-18; discusses selectively distributing alpha-numeric codes, creating a table in the printer to cross-reference private keys with alpha-numeric codes and, wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code.

As per claim 8: See Mazzagatte on col.5, lines 53-65 and col.6, line 62-col.7, line 5; discusses spooling the encrypted documents from the file server to a printer memory, and wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

As per claim 10: See Mazzagatte on col.7, lines 3-56 and col.9, lines 26-34; discussing in response to accepting the private key, generating a list of documents encrypted with the corresponding public key, creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document, and wherein printing the documents includes printing the documents in response to selecting a document.

As per claim 11: See Mazzagatte on col.4, lines 37-40; discusses transmitting a facsimile transmission and wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

As per claim 19:

Mazzagatte discloses communications security system in a network of connected devices, the system comprising:

a computer having a network connection, an input to accept a public key, and an encryption application to supply encrypted documents to the network connection in response to accepting a public key; **(col.4, lines 40-42 and col.9, lines 13-20)**

a network connected to the computer to receive and transmit encrypted documents; and, **(col.3, lines 48-555 and col.8, lines 14-15)**

a file server connected to the network to receive encrypted documents from the computer; and **(col.6, lines 20-21 and col.6, line 62 – col.7, line 5)**

a printer having an input connected to the network to accept encrypted documents from the file server **(col.5, lines 47-50)**, the printer having an input

to accept a private key corresponding to the public key used to encrypt the documents at the computer, the printer having a decryption application to decrypt the documents with the private key **(col.9, lines 13-20)**, and the printer having an output to supply a printout of the decrypted documents. **(col.10, lines 31-39)**

The server of Mazzagatte is a print node (col.7, lines 39-44) which may be a gateway to one or multiple printers (col.10, lines 43-44) or basically a file server (col.4, lines 31-34), where the print node server receives the encrypted data and identification information using public/private key encryption (col.4, lines 40-42) and sends the encrypted data with the private key (col.10, lines 31-33) to the printer for printing (col.6, lines 63-65). The print node and the printer communicates with one another such that the print node indicates the print job information for the printer to determine which recipient is to receive the printouts from the print queue (col.10, lines 13-14). Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric (public/private key) algorithms, Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source, which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify that the user has correct access privileges (col.5, lines 51-65). Part of DeBry's invention involves authenticating the printer prior to allowing the printer to receiving encrypted documents. Thus, DeBry has an

added security measure to make sure the printer is trusted before transmitting the files and thereafter the server have the option using a secret key or a public key to encrypt prior to sending an encrypted file to the user whereby the user decrypts the file using the appropriate key (col.10, lines 16-21). The appropriate key of an asymmetric key scheme can obviously be a private key if the received public key is used for encryption. Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15).

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer because to

prevent unauthorized printing and spoofing.

As per claim 20: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discussing the computer includes printer driver encryption software to generate the encryption application; and wherein the printer is operated in response to the printer driver encryptions software loaded in the computer.

As per claim 21: See col.4, lines 57-58 and col.7, lines 33-55; discussing the computer has a display with an input connected to the application, wherein encryption application creates a graphical user interface (GUI) dialog box on the display to optionally invoke the encryption of documents, and in response to invoking the document encryption option, creates a GUI dialog box to request and accept public key information.

As per claim 22: See Mazzagatte on col.7, lines 11-27; discussing a system administrator to generate a plurality of public keys with corresponding private keys, the system administrator distributing the public keys universally to network-connected computers, and selectively distributing the private keys.

As per claim 23: See Mazzagatte on col.4, lines 9-10 and col.9, line 56; private keys configured as code in SMART cards; and, wherein the printer private key input is a card reader to read SMART cards, the printer using the code read by the card reader as the private key.

As per claim 24: See Mazzagatte on col.4, lines 39-41 and col.10, lines 4-20; discussing the system administrator generates a table cross-referencing the private keys to alpha-numeric codes, and selectively distributes the alpha-

numeric codes; and, wherein the printer private key input is a keyboard interface to accept private keys referenced by the alpha-numeric code entered on the keyboard, and the printer further comprising a memory to store the private keys, and a table to cross-reference private keys to alpha-numeric codes.

As per claim 25: See Mazzagatte on col.6, line 62-col.7, line 5 and col.11, lines 17-20; discussing the printer includes a memory to spool the encrypted documents received from the file server, the printer decrypting the documents with the private key by retrieving the encrypted documents from printer memory.

As per claim 27: See Mazzagatte on col.7, lines 13-67 and col.9, lines 26-34; discussing the printer has display connected to the decryption application to depict a list of documents encrypted with a corresponding public key, in response to accepting the private key; wherein the printer decryption application creates a GUI dialog box on the display to invoke the selection of encrypted documents, the printer printing the documents in response to selecting a document from the GUI dialog box.

As per claim 28: See Mazzagatte on col.4, lines 37-40; discussing the computer transmits the encrypted documents as a facsimile (FAX) transmission; wherein the network is a telephone system; and, wherein the printer decrypts the encrypted FAX transmission.

(10) Response to Argument

The section 103(a) rejection over Mazzagatte, et al. and Debry.

Mazzagatte et al. teach an invention directed to secure printing of image data such that the image data can only be printed on an image forming device in the presence of an intended recipient where the document is securely transmitted from a computer to a remote image forming device in a networked environment **(col.3, lines 44-55)**. The networked computing environment comprises a network which is connected to desktop computer 10, a laptop computer 20, server 40, digital copier 30, and printer 50 wherein the network 100 can be utilized over the internet. Mazzagatte describes the printer 50 as containing a private key corresponding to the printer for encryption/decryption purposes **(col.5, lines 38-42)** and that encryption/decryption logic 355 enables printer to receive encrypted data and enable decryption of the encrypted print data in the presence of the intended recipient **(col.6, lines 15-19)**. The server 40 interacts with the network 100 where the server receives the encrypted data and to either maintain data in queue 415 where queue stores numerous print jobs for output or to send such data to one or more forming device such as the printer 50 for printing **(col.6, line 61 – col.7, line 5)**. Mazzagatte discloses encrypting data prior to transmitting to the receiving networked connected printer using Public Key Infrastructure, symmetric, or asymmetric key infrastructure **(col.8, lines 38-40 and col.9, lines 15-16)**.

Appellants addressed that Mazzagatte does not discuss using a public key to encrypt the print job and also indicated that the Office Action "acknowledges that Mazzagatte does not describe any public key encryption details". Appellants cited Figures 5-7B for supporting these allegations. However, the last Office Action states that "although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric (public/private key) algorithms, Mazzagatte did not specifically describe the details of the encrypted data by using the public key" because Mazzagatte vaguely discloses an asymmetric key (public/private key pair) and emphasized more on the symmetric key technique.

Further, Appellants noted "symmetric key is not a public or a private key, but rather, a secret key" (pages 5-6). Appellant did not provide any citation from any of the prior arts of such allegations. A private key is inherently kept from untrusted users or from trusted users not allowed to gain access to a particular file because not all trusted users are automatically allowed to have access to all of the files. A private key is kept secret from other users from accessing the file, thus evidently is a secret key. The symmetric key is known as having the same key for decryption as the received key of the encrypted document and an asymmetric key is having a different key for decryption from the key of the encrypted document. Therefore, Mazzagatte does not exclude any other cryptography methods that may also be used for decryption in order to print the documents and that the files is encrypted using the symmetric key

or asymmetric key **(col.9, lines 13-14)** and accepting a corresponding (i.e. private) key to the (i.e. public) key of the encrypted documents and decrypting the documents with that (private) key to print the documents **(col.10, lines 31-33)**. However, to further disclose in details the usage of public key encryption and private key decryption of a file, DeBry is brought forth.

DeBry teaches an invention enabling a user or client system 20 to pass authorization to a printer to retrieve and print file from a file source **(col.5, lines 34-36)**. DeBry include file servers **(col.7, lines 4-5)** or a document source, which is the owner of the document **(col.7, lines 50-55)** where the document source creates a certificate to verify that the user has correct access privileges **(col.5, lines 51-65)** and it would be advantageous to provide a unique public encryption key and decrypt and print the document using standard decryption algorithms **(col.10, lines 37-44)**. Part of DeBry's invention involves authenticating the printer prior to allowing the printer to receiving encrypted documents. Thus, DeBry has an added security measure to make sure the printer is trusted before transmitting the files and thereafter the server have the option using a secret key or a public key to encrypt prior to sending an encrypted file to the user whereby the user decrypts the file using the appropriate key **(col.10, lines 16-21)**. The appropriate key of an asymmetric key scheme can obviously be a private key if the received public key is used for encryption. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry

for receiving an encrypted the document with a public key and a private key is used for decryption at the printer because public/private key cryptography prevents unauthorized printing and spoofing.

Appellant appeals that "Mazzagatte's system only encrypts a document at the destination printer" (page 6), but fails to provide any citation for such allegation. Mazzagatte does teach the printer 50 is connected to the network 100 that is able to receive email messages containing print job related information **(col.6, lines 25-28)** and Figure 1, shows the printer is connected to and in communication to the network where the server sends encrypted files to the printer **(col.6, lines 15-19 and 63-65).**

Appellants appeals that "the document is not encrypted using someone else's public key" and that "the decryption cannot be enabled until the user arrives at the printer and enters their private key" (page 7). Further, Appellants indicates the user holds the private key preventing a document from printing until the user presents the private key (page 8). The claimed invention recites receiving documents encrypted with a public key where the limitations does not limit to where the public key is derived from or what is the makeup of this public key and does not restrict any part of the user being at the printer to present the private key in order to decrypt the documents. The claims recites "accepting a private key corresponding to the public key used to encrypt the document" which is very clear that the claims do not specify or limit to

the user presenting the private key. Therefore, Mazzagatte does teach enabling decryption of the encrypted print data with the private key of the private/public key pair for use in encryption/decryption of data, i.e. document received by the printer **(col.6, lines 15-19; col.7, lines 11-34; col.9, lines 31-35; and col.10, lines 31-37).**

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Leynna Ha

Leynna Ha

Conferees:

Kim Vu (SPE) KV

Song Ho (PE) SH